EVOLUCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ESTADO COLOMBIANO

Espitia Ruíz John Jairo.
jespitiaruiz@yahoo.es
Universidad Piloto de Colombia

Resumen—En este artículo trataremos la evolución del Estado Colombiano en los temas referentes a la Seguridad de la Información. Veremos cómo se dieron unos primeros pasos a través de la promulgación de algunas leyes como la Ley 527 de1999 de Comercio Electrónico y la circular 052 de 2007, posteriormente la Ley 1273 de 2009 de delitos informáticos y la Ley 1341 de 2009.

La expedición de estas leyes fue muy útil, pero solo hasta la aparición del CONPES 3701 en el año 2011 se establece la política estatal de Ciberseguridad y Ciberdefensa dándose así la importancia por parte del Estado Colombiano a estos temas como vitales para preservar la seguridad nacional.

Después aparecieron otras leyes como la Ley 1581 de protección de datos personales en el año 2012 y en el año 2014 la Ley de Transparencia y Acceso a la información pública, a la vez que a la estrategia de Gobierno en Línea se le adiciono un modelo para indicar como las entidades territoriales deben implementar el Sistema de Gestión de Seguridad de la Información SGSI.

***Abstract*—**This article will attempt the evolution of the Colombian State in matters relating to information security. We'll see how some first steps were taken through the enactment of some laws such as Law 527 of 1999 on Electronic Commerce and Circular 052 of 2007, then 1273,2009 Law of Computer Crime Act 1341 and 2009.

The issuance of these laws was very helpful, but only until the appearance of CONPES 3701 in 2011 the state policy of Cyber Security and Cyber thus giving states the importance by the Colombian government to these issues as vital to safeguard national security.

Then came other laws such as the 1581 Law on protection of personal data in 2012 and in 2014 the Law of Transparency and Access to Public Information, while the strategy of Government Online was added as a model for indicate how local authorities should implement the Management System ISMS Information Security

Índice de Términos—CONPES 3701, Ley 1581 de 2012, Ciberseguridad, Ciberdefensa, Gobierno en Línea, Seguridad de la Información, Ley de Transparencia y Acceso a la información pública de 2014, Ley 527 de 1999, Ley 1273 de 2009, comercio electrónico.

I. INTRODUCCIÓN

Desde la llegada de Internet a Colombia a mediados de la década de los 90, el número de usuarios y entidades conectados a la red, empezó a crecer a gran escala.

Las empresas empezaron a ofrecer a sus clientes cada vez más servicios electrónicos, empezó a surgir en nuestro país una tendencia mundial denominada "e-commerce" o en español "comercio electrónico".

Con esas novedades tecnológicas, nació también la necesidad de adecuar la estructura jurisprudencial de nuestro país, para incorporar normas que facilitaran el intercambio mercantil a la luz de las nuevas tecnologías. Es así como aparece la Ley 527 de 1999 de comercio electrónico, "en la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación".

En esta ley se define claramente que son los mensajes de datos electrónicos, lo que permite cimentar la jurisprudencia en adelante con respecto a los delitos informáticos.

En el año 2000 se promulga la Ley 599 donde por primera vez se tipifica el "Acceso abusivo a un sistema informático" en su artículo 195.

En el año 2007 la Superintendencia Financiera de Colombia expide la circular 052, con la cual fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios del sector financiero.

En el año 2009 se promulgo la ley 1273 de delitos informáticos, con la cual se otorgó a los jueces de la república de Colombia las herramientas para

penalizar la creciente gama de delitos a través de medios electrónicos o contra estos.

Hasta ese momento, las leyes promulgadas penalizaban algunas de esas conductas delictivas a través de medios electrónicos y normas como la circular 052 operaban sectorialmente, para preservar la seguridad de la información, pero no había una política de Estado al respecto.

Es sólo hasta la creación del documento CONPES 3701 del año 2011 que el Estado Colombiano se interesa por el tema de Seguridad de la Información y es así como se empieza hablar de Ciberseguridad y Ciberdefensa, para preservar la Seguridad Nacional.

Vemos entonces que todas estas leyes tienen en común que pretenden garantizar las tres características de la información, como son la integridad, la disponibilidad y la confidencialidad.

La Seguridad de la Información según el estándar ISO/IEC 27001, aprobado y publicado en octubre de 2005 por la International Organization for Standarization (ISO) y por la comisión International Electrotechnical Comission (IEC) se define como: "La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio."

II. LEY 527 DE 1999

El propósito de esta ley fue reglamentar el marco jurídico para el creciente uso de servicios ofrecidos por entidades para sus clientes a través de canales electrónicos como la red Internet, lo que se conoce como "comercio electrónico". Por tanto esta ley expone el siguiente objetivo "Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones". Ahora veamos algunas definiciones de esta ley.

ARTÍCULO 2. DEFINICIONES. Para los efectos de la presente ley se entenderá por:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.

f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Ahora veamos los artículos donde se otorga el reconocimiento jurídico a los mensajes de datos definidos en esta ley.

ARTÍCULO 5. RECONOCIMIENTO JURÍDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo

tipo de información por la sola razón de que esté en forma de mensaje de datos.

ARTÍCULO 9. INTEGRIDAD DE UN MENSAJE DE DATOS. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

ARTÍCULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original."

Vemos entonces que esta ley otorgó definición legal a los componentes de las relaciones comerciales realizadas a través de medios electrónicos, en su artículo 2º, pero fue más allá y otorgo reconocimiento jurídico y fuerza probatoria a la información contenida en medios electrónicos, en sus artículos 5 y 10 siempre y cuando preserven estos las características de integridad descritas en el artículo 9.

III. LEY 599 DE 2000

Esta ley es el código penal colombiano y encontramos un capitulo con artículos que tipifican delitos relacionados con el uso de tecnologías de la información. Veamos entonces el capítulo.

CAPÍTULO VII. DE LA VIOLACIÓN A LA INTIMIDAD, RESERVA E INTERCEPTACIÓN DE COMUNICACIONES.

ARTÍCULO 192. VIOLACIÓN ILÍCITA DE COMUNICACIONES. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de dieciséis (16) a cincuenta y cuatro (54) meses, siempre que la conducta no constituya delito sancionado con pena mayor. Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de treinta y dos (32) a setenta y dos (72) meses.

ARTÍCULO 195. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

ARTÍCULO 197. UTILIZACIÓN ILÍCITA DE REDES DE COMUNICACIONES. El que con fines ilícitos posea o haga uso de equipos terminales de redes de comunicaciones o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de cuatro (4) a ocho (8) años. La pena se duplicará cuando la conducta descrita en el inciso anterior se realice con fines terroristas.

Vemos entonces que este capítulo tiene definidos los artículos 192,193, 1965 y 197 se hicieron las primeras tipificaciones de delitos informáticos en el código penal colombiano. En el artículo 195 por ejemplo se tipifica el "Acceso abusivo a un sistema informático."

IV. CIRCULAR 052 DE 2007

En esta circular se definen una serie de requerimientos tendientes a robustecer la seguridad y la calidad en el manejo de la información de clientes y usuarios por parte de las entidades vigiladas por la Superintendencia Financiera de Colombia, a través de diferentes medios y diferentes Canales.

Los Canales a los que se hace referencia son: Oficinas, Cajeros Automáticos (ATM), Receptores de cheques, Receptores de dinero en efectivo, POS (incluye PIN Pad), Sistemas de Audio, Respuesta (IVR), Centro de atención telefónica (Call Center, Contact Center), Sistemas de acceso remoto para clientes (RAS), Internet y dispositivos móviles.
Los medios son: tarjetas débito y crédito. Algunos de los requerimientos de la esta circular son:
“

- Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.
- Contar con mecanismos que verifiquen la autenticidad y denominación de los billetes.
- Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados.
- Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.”

Como se puede observar claramente, con estos requerimientos, la Superintendencia Financiera de Colombia, busco asegurar los pilares de Seguridad de la Información, como son la Confidencialidad, la Integridad y la Disponibilidad de la información de los usuarios del sector financiero de nuestro país.

V. LEY 1273 DE 2009

Esta ley es también conocida como la Ley de delitos informáticos y básicamente tipifico nuevas conductas delictivas relacionadas con delitos cometidos haciendo uso de las tecnologías de la información, fijando para ello penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

A continuación los delitos tipificados en el capítulo primero “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” [1].
“**ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO**.

ARTÍCULO 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.

ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

ARTÍCULO 269D. DAÑO INFORMÁTICO.

ARTÍCULO 269E. USO DE SOFTWARE MALICIOSO.

ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES.

ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.”

En resumidas cuentas esta ley permitió la tipificación clara de las conductas delictivas asociadas al creciente uso de las tecnologías de la información.

Por ejemplo el artículo 269G tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que por lo general utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales.

En esta ley también se establecieron claramente las penas carcelarias y las multas en dinero, así como los agravantes de cada uno de los delitos aquí tipificados.

Así pues la Ley 1273 es una herramienta clave en la lucha contra los delitos informáticos en Colombia, porque define claramente las conductas maliciosas que pueden ser realizadas por ciudadanos que tengan acceso a tecnologías de la información.

Por otra parte los jueces de la republica cuentan así con un marco legal que les permite castigar a los delincuentes informáticos, y en general se puede decir que nuestra legislación ya no permite que los actores de ese tipo de conductas delictivas sean excarcelados por vacíos jurídicos. También se incentiva a la sociedad civil y a entidades públicas y privadas a denunciar esta clase de delitos.

VI. LEY 1341 DE 2009

En julio del año 2009, el gobierno expidió la Ley 1341 "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la formación y las comunicaciones – TIC-se crea la agencia nacional de espectro y se dictan otras disposiciones", señala en su artículo dos (2), como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: "la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno en Línea".

Vemos entonces que con la promulgación de esta ley, el gobierno reglamentó las políticas que rigen el sector de las Comunicaciones y las Tecnologías de la Información, en lo relacionado con temas de cobertura, administración del espectro radioeléctrico [2], cobertura y calidad del servicio.

Pero quizás lo más destacable de esta ley es la importancia que se da a los ciudadanos como usuarios de los servicios de Tecnologías de la Información, por eso en su artículo segundo [3] que define los principios orientadores de esta ley, hay varios de ellos enfocados a los usuarios como son los principios 1,3,4,7 y 8.

VII. CONPES 3701 DE 2011

La elaboración de este documento CONPES se llevó a cabo en el año 2011, con la participación de las siguientes entidades del Estado Colombiano:

- Ministerio de Interior y de Justicia
- Ministerio de Relaciones Exteriores
- Ministerio de Defensa Nacional
- Ministerio de Tecnologías de la Información y las Comunicaciones
- Departamento Administrativo de Seguridad
- Departamento Nacional de Planeación
- Fiscalía General

Estas instituciones identificaron que pese a las iniciativas gubernamentales y privadas para enfrentar el creciente número de amenazas cibernéticas, no hay una política estatal que permita el actuar coordinado de todas las entidades nacionales, territoriales y de los ciudadanos, para hacer frente a estas amenazas y garantizar así la Seguridad Nacional a través de la Seguridad de la Información.

Para esto se planteó el siguiente objetivo principal: "Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio."

Como se observa en ese objetivo principal, se introducen los términos Ciberseguridad [4], ciberdefensa [5] y ciberespacio [6].

El principal antecedente que impulsa la creación de este documento es el ocurrido en abril de 2007 al gobierno de Estonia, el cual es considerado el mayor ataque cibernético de la historia y que afecto entre otras entidades a la presidencia, el parlamento y los ministerios. Este incidente requirió la intervención de la Organización del Atlántico Norte OTAN [7] para solventarlo.

Sin duda alguna este incidente hizo que muchos países incluido Colombia, le dieran al tema de Seguridad de la Información la importancia requerida y se incluyera como en el caso de nuestro país en la agenda nacional.

VIII. LEY 1581 DE 2012

La aparición de técnicas como el robo de identidad o "pishing", o la obtención de información de usuarios en redes sociales como Facebook a través de lo que se conoce como Ingeniería Social.

Sin embargo existen otras formas de obtener información como son el diligenciamiento de encuestas en Internet o en los supermercados, o en las recepciones de los edificios.

Todas esas situaciones hacen que el Estado Colombiano, entienda que la información es el activo más importante en el mundo actual, razón por la cual el 17 de octubre de 2012 el gobierno expidió la Ley Estatutaria (ley de especial jerarquía) [8] 1581 [9] "por la cual se dictan disposiciones generales para la protección de datos personales".
Esta ley busca proteger los datos personales registrados en cualquier base de datos y reglamenta también las operaciones que sobre ellos se pueden realizar como son la recolección, almacenamiento, uso, circulación o supresión (en adelante Tratamiento) por parte de entidades de naturaleza pública y privada.

Esta ley busca salvaguardar los derechos de los ciudadanos consagrados en los artículos 15 y 20 de la constitución política de política de Colombia [10] y el derecho fundamental al hábeas data [11].

Se entiende al hábeas data como una garantía del derecho a la intimidad consagrado en la Constitución Política de Colombia, por ello se habla de "la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir."

La Ley obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas, como entidad responsable del tratamiento (persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos) deben definir los fines y medios esenciales para el tratamiento de los datos de los usuarios y/o titulares, incluidos quienes fungen como fuente y usuario, y los deberes que se le adscriben responden a los principios de la administración de datos y a los derechos –intimidad y hábeas data – del titular del dato personal.

IX. LEY 1712 DE 2014

La ley de Transparencia y Acceso a la información Pública concede a los colombianos el derecho fundamental a la información, haciendo énfasis en que los ciudadanos ya no tendrán que pedir información pública de su interés acercándose a las entidades, sino que es el Estado a través de sus diferentes entidades quien debe entregarla, no solamente dando respuesta a peticiones, sino también divulgarla y/o publicarla continuamente según sus actualizaciones, de forma general, de fácil acceso y comprensible, ya sea impresa, por medios masivos de comunicación y las formas de transmisión electrónicas.

Esta ley que promueve la transparencia en la gestión pública inicialmente comenzara a regir para las entidades públicas de orden nacional después de un periodo de 6 meses de haberse aprobado la ley, luego se aplicara en las entidades públicas territoriales dentro de un año. Es de anotar que en la totalidad de las entidades del Estado es obligatorio tener y poner en práctica lo establecido para la publicación y divulgación de gobierno en línea en la estrategia de Gobierno en Línea, contemplando la obligación de publicar información a través del esquema de datos abiertos que estipula la estrategia.

X. GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

Con la expedición de todas las leyes mencionadas en este artículo, el Estado Colombiano estaba tratando el tema de seguridad de la información directa o indirectamente y por tanto temas de Gestión de Riesgos. Con la expedición del decreto 2618 del 2012, se modifica la estructura del Ministerio de las TIC, se crea la Subdirección de Seguridad y Privacidad de TI, la cual tiene funciones claramente estipuladas, a continuación algunas de estas:

- Liderar la implementación en el Estado de plataformas con estándares de seguridad y privacidad de la información en coordinación con las autoridades pertinentes.
- Definir los lineamientos de política y estándares de protección de la información pública, para su preservación en situaciones de desastre.

- Identificar los activos dependientes del ciberespacio así como su regulación y definir el marco funcional y de responsabilidades en la materia, centrándose en la defensa de las infraestructuras críticas, el tejido empresarial y las libertades y derechos individuales, conforme a la ley vigente.

Estas funciones están claramente relacionadas al tema de Gestión del Riesgo, que busca desarrollar procesos que permitan identificar, analizar y controlar los posibles riesgos que puedan afectar la Seguridad de la Información. Por ello se crea el Modelo de Privacidad de la Información, componente de la Estrategia de Gobierno en Línea, que busca precisamente que sea el mismo Estado a través de sus diferentes entidades, quien implemente las políticas, controles y metodologías necesarios para asegurar la Seguridad de la Información. Este modelo trata el tema de Riesgos en sus diferentes componentes como son planificación, implementación, evaluación de desempeño y mejora continua.

XI. CONCLUSIONES

Desde la promulgación de la Ley 527 de 1999 hasta la Ley de Transparencia y Acceso a la Información Pública del 6 de marzo del año 2014, podemos decir que el desarrollo del Estado Colombiano en temas de Seguridad de la Información, ha sido un poco lento, pues desde la llegada de Internet a Colombia a mediados de la década de los 90, se tardó alrededor de 5 años para formular nuestra Ley de comercio electrónico, 12 años para le generación de la circular 052, dos años más para la promulgación de la Ley de delitos informáticos y dos años más hasta el 2011 para que el Estado creara el CONPES 3701 donde se fijó la política de ciberseguridad y ciberdefensa.

La Estrategia de Gobierno en Línea formulo el modelo de Seguridad de la Información, que deben implementar las entidades del Estado, con un plazo máximo hasta el año 2018, vemos entonces que han pasado casi 25 años y no se ha terminado de implementar en la totalidad del Estado las políticas de ciberseguridad y ciberdefensa. Por tal razón se puede concluir que el Estado Colombiano tiene la infraestructura jurídica necesaria para hacer frente a delitos informáticos, protección de datos personales, acceso de los ciudadanos a la información y al uso de Tecnologías de la información, pero aún hay una gran brecha por cubrir para que todas las entidades nacionales y territoriales queden alineadas con las políticas de ciberseguridad y ciberdefensa expuestas en el documento CONPES 3701. Este es sin duda un gran problema, pues hasta tanto todas las entidades del Estado no implementen el Modelo de Privacidad de la Información, propuesto por la Estrategia de Gobierno en Línea, el riesgo de que el Estado sufra ataques que pongan en riesgo la seguridad nacional, es muy alto.

REFERENCIAS

[1] Alcaldía de Bogotá, “Ley 1273 de 2009,” Enero 2009. [Online]. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] http://www.mintic.gov.co/portal/604/w3-article-2350.html

[3] Alcaldía de Bogotá, “Ley 1341 de 2009,” Julio 2009. [Online]. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[4]http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[5] http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[6]http://www.forosdeinformatica.com/index.php?topic=17252.

[7] http://www.significados.com/otan/

[8]http://www.camara.gov.co/portal2011/preguntas - frecuentes/166-ique-son-las-leyes-estatutarias

[9] Alcaldía de Bogotá, “Ley 1581de 2012,” Octubre 2012. [Online]. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[10] Alcaldía de Bogotá, “Constitución Política de Colombia 1991”, 1991. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

[11]http://www.coltefinanciera.com.co/educacion - financiera/habeas-data

Autor.

John Jairo Espitia Ruíz nació en Bogotá en 1974. Ingeniero de Sistemas de la Fundación Universitaria de Popayán del año 2003. Actualmente, se desempeña como Ingeniero de desarrollo Senior, para la compañía Audisoft SAS y realiza estudios de Postgrado en Seguridad Informática en la Universidad Piloto de Colombia